NIST S/MIME V3 Client Profile

Michael Chernick
chernick@nist.gov
+1-301-975-3610

March 8, 2001

NIST S/MIME Profile Status

- Currently Under Development
- Under Review by Selected S/MIME Editors
- Out for Public Comment Late March 2001
- Relatively Short Document (~13 Pages)

Why is NIST Developing S/MIME Client Profile?

- PKI Technology is Maturing
- Focus is Now on Developing Applications
- NIST is Attempting to Help Facilitate Success of Interoperable S/MIME
- If This Project Successful, Other PKI Applications Will be Profiled

Purpose of S/MIME Profile

- To Identify Subset of S/MIME V3 Specifications That:
  - Helps to Assure Interoperability
  - Promotes Secure Communications at Reasonable Cost
  - Serve as Basis for Test Development
- As Guidance for COTS Product Procurement and Development

S/MIME Profile Sections

- Introduction
- S/Mime Profile Requirements
- Support For Enhanced Security Services (RFC2634)
- Optional Features and Notes on Testing
- References
- Annex on Cryptographic Algorithms (Non-Normative)

S/MIME Profile Requirements(1)

- Mandatory Parts of RFCs 2630, 2632, and 2633
  - Except Diffie-Hellman Key Agreement and DSA not required
- FIPS 140-1 Approved Software Modules
- Mandatory Algorithm Suite
  - RSA (V1.5, RFC2313) Digital Signature,
  - RSA (V1.5, RFC2313) Key Transport,
  - Triple-DES for Content Encryption,
  - SHA-1 Hash Algorithm
  - RSA Key Size at least 1024 bits

S/MIME Profile Requirements(2)

- Recommended Additional Algorithm Suites
  - RSA, RSA, SHA-1, AES
  - DSA, D-H, SHA-1, Triple-DES (DSA & D-H as in RFC 2630)
  - DSA, D-H, SHA-1, AES (DSA & D-H as in 2630)
- Other Crypto Algorithms OK (e.g., ECDSA) for Interoperability and Backward Compatibility (Especially FIPS 140-1 Approved), But Caution on Older/Weaker Algorithms

S/MIME Profile Requirements(3)

- PKIX (RFC 2459) Conformance Required
- Federal PKI X.509 Cert. And CRL Extensions Profile (twg-00-18.xls) Conformance Required
- Generation and Reception of these CMS Content Types (Defined in RFC 2630)
  - Data
  - SignedData
  - EnvelopedData
- Conforming Implementations Must be Capable of Processing Nested Content Types

MSG Generation Rqmts. (1)

- Implementations Must Be Able To Generate Correctly Formatted Messages
- Sending Signed Messages
  - Must Be Able to Generate/Include SignerInfo, SMIMECapabilities Attribute, User Certs and CRLs, Multipart/Signed (i.e., “clear”) msgs

MSG Generation Rqmts. (2)

- Sending Encrypted Messages
  - Must Be Able to Generate Symmetric keys, Encrypt Msgs. Using Them, and Encrypt Symm. Keys Using PKCS#1 V1.5 (RSA as in RFC 2313)
  - Must Be Able to Encrypt for Multiple Recipients
  - Must Be Able to Construct & Validate Cert. Path for Receiver's Key Mgmt. Cert. & CRLs Using LDAP (or Reject Cert.)
  - "Should" Be Able to Generate D-H Keys and Derive KEKs as Defined in RFC 2631

MSG Generation Rqmts. (3)

- Sending Signed and Encrypted Messages
  - Must Be Able to Support Signed Message Requirements
  - Must Be Able to Support Encrypted Message Requirements
  - When Sender Supports More Than One Key Mgmt. Method, SMIMECapabilities Should be Used to Automatically to Select a Method

MSG Generation Rqmts. (4)

- Must Be Able to Generate Return Signed Receipt Messages
- Must Be Able to Request Return Receipt in Both Signed and Unsigned Messages
- Must Be Able to Create Properly Formatted MIME Headers as per RFC2633

MSG Reception Rqmts. (1)

- Must Be Able to Receive and Process S/MIME Messages that are Correctly Formatted
- Recipients Must Be Able to Verify Signature or Decrypt Data Using Info. Provided by the Sender
- Must Be Able to Process Properly Formatted MIME Headers as per RFC2633

MSG Reception Rqmts. (2)

- Receiving Signed Messages
  - Implementations Must Be Able to Process SMIMECapabilities Attribute
  - Must Be Able to Process SignerInfo Including Signed Attributes
  - Must Be Able to Process Both “Clear” & “Opaque” signed Messages
  - Must Be Able to Acquire Certs. By Extraction From Incoming Messages

MSG Reception Rqmts. (3)

- Receiving Signed Messages (Continued)
  - Must Be Able to Handle Unknown Attributes "Gracefully" by
    - Reject Msg. & Inform the User
    - Accept Msg. & Inform the User
    - Provide the User with an Option to Reject or Accept
  - Must Be Able to Construct Cert Path for Sender's Cert., Including CRLs, using LDAP
  - Must Validate Cert. Path to End Cert. That is Signers' Cert. or Reject Cert.

MSG Reception Rqmts. (4)

- Receiving Signed Messages (Continued)
  - Must Ensure that either the SubjectAltName.rfc822Name or PKCS#9 emailAddress in the signer's certificate matches the actual email address used in the received message's “From” or “Sender” field (See [RFC2459] and [RFC2632]). If the addresses do not match, the S/MIME implementation MUST display information to the user to allow the user to accept or reject the message.

MSG Reception Rqmts. (5)

- Receiving Encrypted Messages
  - Implementations Must Be Able to Process Encrypted Messages Including Recovery of Symmetric Key and Using It to Decrypt the Message
  - Should Allow a Transparent Selection of Appropriate Private Key for Decryption of an Incoming Message When Recipient Has Multiple Certs. (Each Associated with a Private Key) Used for Key Management

MSG Reception Rqmts. (6)

- Receiving Signed And Encrypted Messages
  - Implementations Must Be Able to Support Signed Message Requirements
  - Implementations Must Be Able to Support Encrypted Message Requirements
  - Must BE Able to Process Return Signed Receipt

Certificate Processing(1)

- Must Be Able to Process All Critical or Optionally Critical Cert. Extension in Federal Cert. & CRL Profile.
- Must Not Reject Certs. With Unrecognized Non-Critical Extensions
- Should Be Able to Support Distinct Certs. For Signing and Key Mgmt. Security Services
- Must Be Able to Process All Critical or Optionally Critical Extensions CRL Extensions in Fed. Cert. & CRL Profile
- Must Not Reject CRLs With Unrecognized Non-Critical Extensions

Certificate Processing(2)

- Must Be Able to Perform Path Validation According to RFC 2459, Section 6.
- Must Be Able to Use X.509 CRLs to Establish Cert. Status for Path Validation At Minimum the Following Aspects Must Be Implemented:
  - Cert. Policies, Policy Constraints, and Policy Mapping
  - Basic Constraints
  - DSA Parameter Inhertitance if DSA is Supported
  - Processing Cert. Paths with Multiple Signature Algorithms
  - Name Chaining, Signature Verification, Validity Date Checking, Revocation Checking, Key Usage/Extended Key Usage, CRL Distribution Points, and CRL Extensions & CRL Entry Extensions

Certificate Processing(3)

- Implementations Must Be Able to Construct Cert. Paths Between Accepted Trust Points and Sender's or Recipient's Certs.
- The Following Features Must Be Supported:
  - Use of Directory Systems
  - LDAP Referrals
  - Use of PKIX Authority Information Access (AIA) Extension
  - CRL Distribution Point Extensions
  - Cross Certificate Pairs
  - CA Certificates

Support For Enhanced Security Services (RFC 2634) (1)

- Signed Receipts
  - Agents MUST be Able to Request, Generate, and Process Signed Receipts as per 2634
  - Support of mlExpansionHistory and mlReciptPolicy Attributes are Out of Scope For This Profile
  - Limited to Single Originator (Mail List Processing is Out of Scope)
  - Msg. Originators Must be Able to Generate Signed Receipt Requests
  - Msg. Receivers Must be Able to Generate Signed Receipts
  - Msg. Receivers Must be Able to process Signed Receipts (Including Signature Verification)

Support For Enhanced Security Services (RFC 2634) (2)

- Security Labels
  - Support for Security Labels is Optional, But If Support Claimed Then the Following Requirements are Imposed on Implementation:
    - Msg. Originators Must Be Able to Generate Security Labels as Defined in RFC 2634
    - Agents Must Be Able to Display Security Labels in Received Msgs. as Defined in 2634. Agents Must Be Able to Examine Label and Determine if Recipient is Allowed to See Contents Or Reject Msg.
    - Generation and Support of Equivalent Security Labels is Out of Scope
- Secure Mailing Lists
  - Out of Scope For This Profile (But May Be Added in Future Profile)
- Signing Certificate Attribute
  - If Support Claimed, Senders Must Be Able to Generate Msgs. with Signing Cert. Attributes as Defined in RFC 2634
  - If Support Claimed, Receivers Must Be Able to Properly Process Msgs. with Signing Cert. Attributes as Defined in RFC 2634

Optional Features and Testing Notes (1)

- Optional Features
  - Sending Agents SHOULD Be Able to Generate “Opaque” Messages
  - Snd. & Rec. Agents SHOULD support Self-Signed Certs.
  - Sending Agents SHOULD Be Able to Include “Appropriate” CRLS in Outgoing Messages
  - Agents SHOULD Be Able to Selectively Trust Certs.
  - Agents SHOULD Be Able to Acquire Certs. From *.p7c and *.p7m Files (*.cer and *.crt Files Also Desirable)
  - SHOULD Be Able to Lookup Certs. in LDAP Repositories
  - SHOULD Be Able to Import & Export PKCS#12 Credentials

Optional Features and Testing Notes (2)

- Testing Limitation
  - Some Testing Requires "Human Scoring" Because a User Interface is Involved (e.g., Display of Labels)
- Scope of Profile
  - Security of Operating System and Email Mechanisms are Beyond the Scope of This Profile. Only the Security Aspects of IETF Developed S/MIME Extensions are Addressed.

References and Annex on Cryptographic Algorithms

- Reference Section (Of Course!)
- Cryptographic Algorithm Annex
  - Non-Normative (Strictly Informative)
  - One-Way Hash Algorithms (e.g., SHA-1, SHA-256)
  - Symmetric Encryption Algorithms (e.g., 3DES, AES)
  - Digital Signature Algorithms (e.g., RSA, DSA)
  - Key Mgmt. Algorithms (e.g., RSA, D-H)
  - Algorithm Suites (e.g., SHA-1 (for Message Digest), RSA (Dig. Sign.), RSA (Key Transport), and 3DES (Content Encryption))

Automated S/MIME Test Facility

- Developing Internet-based Automated Testing Facility
- Web Based Info. & Instructions, But Will Use SMTP for Testing
- Support for Both Originator and Recipient Roles (May Require "Human Scoring" & Self-Scoring for Some Tests)
- Help To Ensure Conformance to S/MIME V3 Profile
- Help To Provide Feedback to NIST on Profile and to Developers on Software Feature Omissions, Bugs, etc.
- Possible Feedback To IETF on Errors/Ambiguities in RFCs
- Using Getronics S/MIME Freeware Library (SFL) as Reference Implementation
- Test Scenarios Intended to Cover Profile Requirements and Options (But NOT Out-of-Scope S/MIME Features)

More Information

- **NIST S/MIME Page**

  http://csrc.nist.gov/pki/smime

- **Point of Contact**
  - **Michael Chernick** **chernick@nist.gov**
    +1 301-975-3610